

WHAT IS CLAIMED IS:

1 1. An information security system comprising:
2 plural information resources distributed amongst and executable on one or more
3 servers coupled via a communication network to a client entity, the plural
4 information resources having associated trust level requirements;
5 a gatekeeper interposed between the client entity and the information resources;
6 and
7 a credential gathering service common to the plural information resources,
8 wherein upon receipt of a first request for access to a first of the plural
9 information resources without prior authentication to a sufficient trust
10 level, the gatekeeper redirects the first request to the common credential
11 gathering service and the common credential gathering service obtains a
12 login credential for the client entity in accordance with a mapping rule
13 establishing a correspondence between the sufficient trust level and a set
14 of suitable credential types.

1 2. An information security system, as recited in claim 1,
2 wherein the first request without prior authentication includes an initial request
3 for access to the first information resource.

1 3. An information security system, as recited in claim 1,
2 wherein the first request without prior authentication includes a subsequent
3 request for access to the first information resource, the subsequent request
4 for access requiring a higher trust level than an initial access request.

1 4. An information security system, as recited in claim 1,
2 wherein upon receipt of a second request for access to a second of the plural
3 information resources, the second request is serviced without redirection
4 to the credential gathering service, the second information resource having

5 a trust level requirement no greater than that of the first information
6 resource.

1 5. An information security system, as recited in claim 1,
2 wherein the correspondence established by the mapping rule is a function of
3 session environment information.

1 B 6. An information security system, as recited in claim 5,
2 wherein the session environment information includes one or more of connection
3 speed, source domain, HTTP environment information, browser type,
4 authentication type, request method, MIME typing, user agent, referrer
5 identity, date and time.

1 7. A credential gathering service providing a single sign-on for sessions that
2 potentially include access to plural information resources having differing security
3 requirements, the credential gathering service comprising:

4 an input port configured to receive an access request identifying an initiating
5 client entity;

6 means for associating a trust level requirement with the access request;

7 an encoding of correspondence between trust levels and credential types;

8 selection logic for selecting in accordance with the encoding, a credential type
9 corresponding to the trust level requirement; and

10 a credential obtaining interface for requesting and receiving a credential of the
11 selected credential type for the initiating client entity.

1 8. A credential gathering service as in claim 7,

2 wherein the credential obtaining interface is with the initiating client entity.

1 9. A credential gathering service as in claim 7,

2 wherein the credential obtaining interface is with a credentialing authority.

1 10. A credential gathering service as in claim 7,
2 wherein the credential obtaining interface is with a credentialing device selected
3 from the set of retinal scan device, a voiceprint analysis device, a
4 fingerprint analysis device, and a card reader.

1 11. A credential gathering service as in claim 7, further comprising:
2 an authentication interface for authenticating the received credential.

1 12. A credential gathering service as in claim 11,
2 wherein the authentication interface includes a communications interface to an
3 authentication service with one or more pluggable authentication modules
4 corresponding to the credential types.

1 13. A credential gathering service as in claim 7,
2 wherein the initiating client entity is not initially authenticated to a trust level
3 required by a first of the information resources; and
4 wherein an attempted access to the first information resource by the initiating
5 client entity is redirected to the credential gathering service with an
6 associated trust level requirement corresponding to that required by the
7 first information resource.

1 14. A credential gathering service as in claim 13,
2 wherein the initiating client entity is not initially authenticated.

1 15. A credential gathering service as in claim 7,
2 wherein the log-on request and associated trust level requirement are supplied by
3 the initiating client entity.

1 16. A credential gathering service as in claim 7,
2 wherein the trust level requirement is supplied by the initiating client entity.

1 17. A credential gathering service as in claim 7,
2 wherein the initiating client entity is one of an application and a user.

1 18. A credential gathering service as in claim 7,
2 wherein the credential types include at least two of passwords, certificates,
3 username/password pairs, one time passwords, biometric indicia, and
4 smart cards.

1 19. A credential gathering service as in claim 7,
2 wherein more than one credential type corresponds to a given trust level.

1 20. A credential gathering service as in claim 7,
2 wherein the correspondence between trust levels and credential types is dynamic
3 and the encoding thereof is updateable.

1 21. A credential gathering service as in claim 7,
2 wherein the set of credential types and corresponding trust levels is dynamic and
3 the encoding thereof is updateable.

1 22. The credential gathering service of claim 7, encoded in a machine readable
2 medium as software executable in a networked computing environment to provide the
3 plural information resources with the single sign-on.

1 23. The credential gathering service of claim 22, wherein the machine readable
2 medium is selected from the set of a disk, tape or other magnetic, optical, or electronic
3 storage medium and a network, wired, wireless or other communications medium.

1 24. A method of providing a single sign-on for plural information resources, the
2 method comprising:
3 associating credential types with trust levels;

4 specifying for each information resource, required ones of the trust levels for
5 accesses thereto;
6 obtaining at least one credential corresponding to a client entity and
7 authenticating the client entity thereby; and
8 permitting access to any of the information resources having a specified trust level
9 requirement commensurate with the trust level associated with the
10 authenticated at least one credential.

1 25. A method, as recited in claim 36, further comprising:
2 denying access to any of the information resources having a specified trust level
3 requirement greater than with the trust level associated with the
4 authenticated at least one credential.

1 26. A method, as recited in claim 36, further comprising:
2 for access to any of the information resources having a specified trust level
3 requirement greater than the trust level associated with the authenticated at
4 least one credential, obtaining at least one additional credential
5 corresponding to a client entity and authenticating the client entity
6 thereby;
7 the at least one additional credential having an associated trust level
8 commensurate with specified trust level requirement.

1 27. A method, as recited in claim 36,
2 wherein the credentials types include at least two of passwords, certificates,
3 username/password pairs, one time passwords, biometric indicia, and
4 smart cards.

1 28. A method of providing sign-on in a networked information environment, the
2 method comprising:
3 directing a request for access to a first information resource from an insufficiently
4 authenticated client entity to a credential gathering service;

2 wherein the associating is a function of at least resource identifier and
3 environment information.

1 36. A method of providing a security interface common to plural information
2 resources, the method comprising:
3 associating credential types with trust levels;
4 specifying for each information resource, a required one of the trust levels for
5 accesses thereto;
6 with a login service common to the plural information resources, obtaining at
7 least one credential corresponding to a client entity and authenticating an
8 identity of the client entity thereby;
9 granting or denying access to a first of the information resources based on
10 correspondence between the required trust-level therefor and an
11 authenticated trust level associated with the obtained at least one
12 credential; and
13 granting or denying access to a second of the information resources based on
14 correspondence between the required trust-level therefor and the
15 authenticated trust level.

1 37. A method, as recited in claim 36,
2 wherein the at least one credential is selected from a set of credential types with
3 associated authentication modules.

1 38. A method, as recited in claim 36,
2 wherein differing trust levels are required for access to the first and second
3 information resources.

5 associating a first trust level requirement with the access to the first information
6 resource;
7 selecting from plural credential types, a credential type having an associated trust
8 level commensurate with the first trust level requirement;
9 obtaining a credential of the selected credential type for the client entity; and
10 authenticating the obtained credential.

1 29. A method, as recited in claim 28, the method further comprising:
2 proxying the access request upon successful completion of the authenticating.

1 30. A method, as recited in claim 28, the method further comprising:
2 supplying a cryptographically secured session token to the client entity based on
3 the authenticated credential.

1 31. A method, as recited in claim 28, the method further comprising:
2 after successful completion of the authenticating, proxying a second access
3 request without additional authentication.

1 32. A method, as recited in claim 31,
2 wherein the second access request is directed to the first information resource.

1 33. A method, as recited in claim 31,
2 wherein the second access request is directed to a second information resource, a
3 second trust level requirement associated with access thereto being no
4 greater than the first trust level requirement.

1 34. A method, as recited in claim 28,
2 wherein the associating is by a mapping rule encoded as one or more of a static or
3 dynamic table, a hierarchy of predicates, weighted logic and fuzzy sets.

1 35. A method, as recited in claim 28,